What is claimed is:

1. In a cryptographic system wherein a certifying authority issues digital certificates identifying users of said system, said digital certificates being digitally signed with a private key of said certifying authority to form a digital signature and requiring a public key of said certifying authority in order to verify said digital signature, and wherein a user transaction in said cryptographic system requires verification by a recipient of said user transaction, said verification based on information in said digital certificates and requiring said public key, a method of controlling access to said public key comprising the steps of:

denying access to said public key;

providing said recipient with at least one message containing rules of said system, said rules including maintaining secrecy of said public key;

by said recipient, digitally signing said at least one document, by which said recipient agrees to said rules; and

in response to said digital signing, permitting said recipient to utilize said public key.

2. A method as in claim 1 wherein said step of providing includes the step of providing said recipient with a secure device containing said public key, wherein said public key cannot be obtained from said secure device.

3. A method of enforcing a security policy in a cryptographic system, said policy requiring controlling

access to a public key, said method comprising the steps of:

denying access to said public key;

providing a recipient with a message containing rules of said cryptographic system, said rules including maintaining secrecy of said public key;

by said recipient, digitally signing said document, by which said recipient agrees to said rules;

in response to said digitally signing, permitting said recipient to utilize public key.

4. A method of enforcing a security policy in a cryptographic system, said policy requiring controlling access to a public key, said method comprising the steps of:

providing a recipient with a document containing rules of said system and with a secure device containing an inactive form of said public key, wherein said public key cannot be obtained from said device;

by said recipient, digitally signing said document;

in response to said digital signing, activating said public key in said secure device.

5. A method of enforcing a security policy in a cryptographic system, said policy requiring controlling access to a public key of a certifying authority, said method comprising the steps of:

by said certifying authority,

providing a user with a message containing rules of said system and with a secure device containing an inactive form of said public key, wherein said public key cannot be obtained from said device;

by said user,

indicating an intent to follow said rules, said indicating including the steps of:

hashing said message to obtain a hashed document;

digitally signing said hashed document to form a digital agreement; and

returning said digital agreement to said certifying authority;

in response to said indicating by said user,

by said certifying authority, activating said public key in said secure device.

6. A method as in any one of claims 1-5 wherein each user of the system has a private key, and wherein said rules include at least one of rules requiring payment to a third party upon:

each use of said public key;

each use of a user's private key;

each certification of a certificate's status; and

each confirm-to transaction by a user.

7. A method as in any one of claims 1-5 wherein said rules include rules to pay for use by said recipient of intellectual property used in creating or operating the system.

8. A method as in claim 1 wherein said user transaction is invalid until said step of digital signing is performed.

9. A method as in claim 1 further comprising the steps of:

in response to said signing by said recipient, said certifying authority accepting a transaction from said recipient, said transaction based on said user transaction.

10. In a cryptographic system wherein a certifying authority issues digital certificates identifying users of said system, said digital certificates being digitally signed with a private key of said certifying authority to form a digital signature and requiring a public key of said certifying authority in order to verify said digital signature, and wherein a user transaction in said cryptographic system requires verification by a recipient of said user transaction, said verification based on information in said digital certificates and requiring said public key, a method of controlling access to said public key comprising the steps of:

providing said recipient with a secure device containing an inactive form of said public key, wherein said public key cannot be obtained from said secure device;

in response to a predetermined transaction with said secure device, activating said inactive public key is said secure device, said predetermined transaction including information from the secure device identifying operational capabilities of the secure device and uniquely identifying said secure device and further including information uniquely binding said recipient to said predetermined transaction.

11. In a cryptographic system wherein a certifying authority issues digital certificates identifying users of said system, said digital

certificates being digitally signed with a private key of said certifying authority to form a digital signature and requiring a public key of said certifying authority in order to verify said digital signature, and wherein a user transaction in said cryptographic system requires verification by a recipient of said user transaction, said verification based on information in said digital certificates and requiring said public key, a method of controlling access to said public key comprising the steps of:

providing said recipient with a secure device;

in response to a predetermined transaction with said secure device, transferring said public key to said secure device, said predetermined transaction including information from the secure device identifying operational capabilities of the secure device and uniquely identifying said secure device and further including information uniquely binding said recipient to said predetermined transaction, wherein said public key cannot be obtained from said secure device.

12. A method as in one of claims 10 and 11 wherein said public key in said secure device becomes inactive after a predetermined time period, said method further comprising the steps of:

after said public key in said device becomes inactive,

in response to another predetermined transaction with said secure device, activating said inactive public key is said secure device, said other predetermined transaction including information from the secure device identifying operational capabilities of the secure device and further including information

uniquely binding said recipient to said other predetermined transaction.

13. A method of enforcing a policy in a cryptographic communication system comprising the steps of:

forming a digital message by a user;

combining with said message at least one user rule;

forming a digital user signature based on said digital message, said at least one user rule and a private key of said user;

combining said digital message, said at least one user rule and said digital user signature to form a digital user transaction; and

combining with said digital user transaction a digital identifying certificate issued by a certifying authority, said identifying certificate having a plurality of digital fields, at least one of said fields identifying said user, wherein

said at least one user rule specifying conditions under which said digital message transaction is valid.

14. A method as in claim 13, further comprising the step of:

combining with said digital transaction a digital authorizing certificate, separate from said identifying certificate and issued by a sponsor of said user for authorizing transactions by said user.

15. A method of enforcing a policy in a cryptographic communication system comprising the steps of:

receiving a digital user transaction including a digital message, at least one user rule specifying conditions under which said transaction is valid and a digital user signature based on said digital message, said at least one user rule and on a private key of a user;

receiving a digital identifying certificate issued by a certifying authority and having a plurality of digital fields, at least one of said fields identifying said user;

verifying said transaction based on information in said certificate and in said at least one user rule; and

accepting said transaction based on said outcome of said verifying.

16. A method as in claim 15, further comprising the step of:

receiving a digital authorizing certificate, separate from said identifying certificate and issued by a sponsor of said user and authorizing transactions by said user; and wherein said step of verifying includes the step of:

verifying said transaction based on information in said authorizing certificate.

17. A method as in any one of claims 13-16 wherein said at least one user rule includes at least one of:

(a) allowed document types of said transaction;

(b) allowed locations at which transactions can be formed;

(c) allowed times at which transactions may be formed;

(d) a time period within which said signature is valid;

(e) a monetary limit for said transaction; and

(f) co-signer requirements for said transaction.